Vulnerability Digest

May 2020

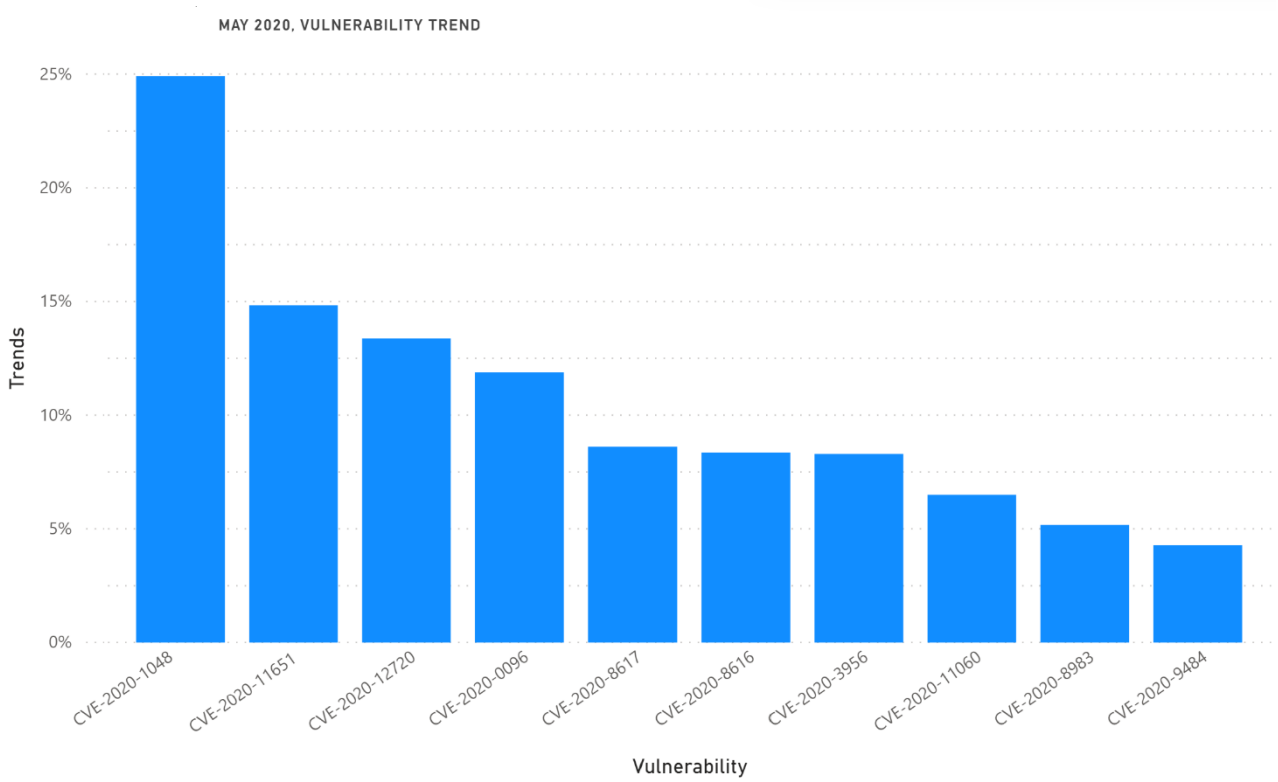
ScanTitan is security scanner and threat intelligence solution that aims to reduce attack surface and cyber security exposure for public services.

Papendrecht 318 3351, Netherlands | info@scantitan.com

SUMMARY

This report shows the monthly top 10 trends on security vulnerabilities and how hackers, malware and exploit kits are exploiting those vulnerabilities. We assign trend value as a percentage of how each vulnerability is gaining the attention of cyber security communities, attackers and malware. Companies can benefit from the report to have more cyber threat insights and anticipate attacks wave that might target their public assets in the following months.

The following chart shows the trends.



In May 2020, we see that the information security community pays more attention to Microsoft published vulnerabilities as CVE-2020-1048, which is not the most critical, gained the most trends. This vulnerability gained almost 25% of overall May trends.

The next in line is the critical and exploitable SaltStack RCE vulnerability titled as CVE-2020-11651. Other critical and exploitable is the SQL Injection in vBulletin titled as CVE-2020-12720.

CVE	Vulnerability	Publish Date	Exploited	Trends*
CVE-2020-1048	Windows print spooler service elevation	21/05/2020	No	24%
CVE-2020-11651	SaltStack RCE	01/05/2020	Yes	14%
CVE-2020-12720	vBulletin SQL Injection	07/05/2020	Yes	13%
CVE-2020-0096	Android 8/9 elevation	14/05/2020	No	13%
CVE-2020-8617	BIND denial of service	19/05/2020	Yes	11%
CVE-2020-8616	BIND denial of service	19/05/2020	Yes	10%
CVE-2020-3956	VMware Cloud Directory RCE	20/05/2020	No	8%
CVE-2020-11060	GLPI command execution	12/05/2020	No	7%
CVE-2020-8983	Citrix Storage Zones RCE	07/05/2020	No	7%
CVE-2020-9484	Tomcat deserialization code execution	20/05/2020	Yes	6%

*Trends value is rounded.

Subscribe to this monthly report by clicking here and prioritize your efforts on defending against cyber security attacks and threats.

CVE-2020-1048

Publish Date 21/05/2020

Exploited No

CVSSv3 Rate 7.8 HIGH

Description

An elevation of privilege vulnerability exists when the Windows Print Spooler service improperly allows arbitrary writing to the file system. An attacker who successfully exploited this vulnerability could run arbitrary code with elevated system privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Links

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1048

CVE-2020-11651

Publish Date 01/05/2020

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.

Links

http://packetstormsecurity.com/files/157560/Saltstack-3000.1-Remote-Code-Execution.html

https://docs.saltstack.com/en/latest/topics/releases/2019.2.4.html

CVE-2020-12720

Publish Date 07/05/2020

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

SQL Injection in vBulletin before 5.5.6pl1, 5.6.0 before 5.6.0pl1, and 5.6.1 before 5.6.1pl1 where it has incorrect access control.

Links

https://forum.vbulletin.com/forum/vbulletin-announcements/vbulletin-announcements_aa/4440032-vbulletin-5-6-1-security-patch-level-1

https://packetstormsecurity.com/files/157716/vBulletin-5.6.1-SQL-Injection.html

CVE-2020-0096

Publish Date 14/05/2020

Exploited No

CVSSv3 Rate 7.8 HIGH

Description

In startActivities of ActivityStartController.java, there is a possible escalation of privilege due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-8.0 Android-8.1 Android-9.

Links

https://source.android.com/security/bulletin/2020-05-01

CVE-2020-8617

Publish Date 19/05/2020

Exploited Yes

CVSSv3 Rate 7.8 HIGH

Description

Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state (DoS) if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable.

Links

https://packetstormsecurity.com/files/157836/BIND-TSIG-Denial-Of-Service.html

https://kb.isc.org/docs/cve-2020-8617

CVE-2020-8616

BIND

Publish Date 19/05/2020

Exploited Yes

CVSSv3 Rate 8.6 HIGH

Description

In BIND DNS Server, a malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral.

Links

https://kb.isc.org/docs/cve-2020-8616

http://www.nxnsattack.com/

CVE-2020-3956

vmware

Publish Date 20/05/2020

Exploited No

CVSSv3 Rate 8.8 HIGH

Description

VMware Cloud do not properly handle input leading to a code injection vulnerability. An authenticated actor may be able to send malicious traffic to VMware Cloud Director which may lead to arbitrary remote code execution. This vulnerability can be exploited through the HTML5- and Flex-based UIs, the API Explorer interface and API access.

Links

https://www.vmware.com/security/advisories/VMSA-2020-0010.html

CVE-2020-11060

Publish Date 12/05/2020

Exploited No

CVSSv3 Rate 8.8 HIGH

Description

In GLPI before 9.4.6, an attacker can execute system commands by abusing the backup functionality. Theoretically, this vulnerability can be exploited by an attacker without a valid account by using a CSRF. Due to the difficulty of the exploitation, the attack is only conceivable by an account having Maintenance privileges and the right to add WIFI networks.

Links

https://github.com/glpi-project/glpi/security/advisories/GHSA-cvvq-3fww-5v6f

CVE-2020-8983

Publish Date 07/05/2020

Exploited No

CVSSv3 Rate 7.5 HIGH

Description

An arbitrary file write issue exists in all versions of Citrix ShareFile StorageZones (aka storage zones) Controller, including the most recent 5.10.x releases as of May 2020, which allows remote code execution.

Links

https://support.citrix.com/article/CTX269106

CVE-2020-9484

Publish Date 20/05/2020

Exploited Yes

CVSSv3 Rate 9.8 CRITICAL

Description

Remote Code Execution (RCE) exists in Apache Tomcat where, in certain conditions, an attacker can send a maliciously-constructed request to cause a deserialisation code execution vulnerability.

Links

https://lists.apache.org/thread.html/rf70f53af27e04869bdac18b1fc14a3ee529e59eb12292c8791a77926@%3Cusers.tomcat.apache.org%3E

https://github.com/IdealDreamLast/CVE-2020-9484/